Executive Summary

The MIS Division of the Office of the State Auditor is charged with four primary objectives:

- Provide Information Technology services including operational support, application development, infrastructure management and information security to agency personnel
- Oversight of Senate Bill 991 compliance
- Enterprise Information Technology strategic planning for the Agency
- Information Technology tactical implementation in order to increase productivity, efficiency and security of critical business functions.

In addition to providing for the daily operational support for Agency personnel, the MIS Division completed a number of major projects to enhance the efficiency, quality of service, and security of the Agency.

MIS worked closely with the Office of the State Controller to ensure the Agency met all technical requirements for the Beacon Project (statewide payroll application implemented in March 2008). MIS also worked with ITS and the Enterprise Data Warehouse service (as the first customer of the new Statewide Enterprise level service) to complete the Management Services and Nongovernmental Compliance Division's Grants Compliance online application (Grants Information Center or GIC), greatly enhancing the operational capabilities of that Division. MIS has completed an internal upgrade of the Agency Intranet, completing a change over from a dynamic site to an industry standard portal technology designed to encourage collaboration among personnel and to enable a more efficient workflow during audits. In conjunction with the portal upgrade, MIS piloted an e-Learning initiative to make training more efficient and cost effective.

In addition, MIS has upgraded the Agencies network infrastructure to meet ESAP requirements. MIS will continue to work closely with ITS to securely merge the OSA network infrastructure into the State of North Carolina's architecture.

Two major initiatives are planned for the coming biennium. The first is enhancing and improving the backup, restore and recovery of all Agency data and applications. Review and testing of current applications as well as the BCP/COOP plans has revealed inadequacies in the Agencies current processes and procedures, and these must be corrected.

Secondly, we must replace the current networking infrastructure. The current network switches are running beyond their life expectancy, and in fact are no longer supported by the vendor. In addition, newer network switches will allow us to improve network security as recommended by the 2006 Security Assessment – for example, by running SNMP version 3 instead of version 1.

In addition to the major initiatives, the MIS Division will continue to aggressively work to provide technologies to Agency personnel that will improve the efficiency and quality of Agency critical business functions. MIS will continue to work with the Beacon Project Team to help develop guidelines and requirements for additional Beacon initiatives including the SAP Grants module implementation. The Grants Information Center application for the Management Services and Nongovernmental Compliance Division will be enhanced to improve both usability and functionality. Agency personnel will complete comprehensive training on the new internal portal. The e-Learning system will be expanded by incorporating an advanced Learning Management System solution. This will lead to expanded education and training opportunities including the ability to make vital information available via web casting. In addition, an Agency wide e-Recruiting solution will be designed and implemented to assist in the recruitment and hiring of quality candidates for open Agency positions. An improved Intrusion Prevention System (IPS) will be installed and configured and infrastructure and security needs will continue to be assessed and improved where feasible.

Agency servers and software are maintained and upgraded to latest versions. The Business Continuity Plan (BCP) / Continuation of Operations Plan (COOP) are continuously reviewed and tested to meet State requirements and to address Pandemic influenza planning requirements.

Finally, OSA has been scheduled for ITS consolidation in 2009 and MIS will work with ITS to ensure that required IT services are smoothly transitioned to ITS while maintaining the operational functionality required for OSA to perform its mission.

Major Factors Influencing the Plan

Agency Mission Statement

The Office of the State Auditors mission is to provide state agencies, the legislature and the people of North Carolina with professional, independent evaluations of the State's fiscal accountability and public program performance. We continually strive to ensure that our state government executes its management responsibilities in compliance with applicable laws, rules, regulations, and policies. We also evaluate management controls and policies in an effort to assist state agencies in making more efficient and effective use of public resources.

A. Major Business Initiative – Audit Watch

In today’s environment, as legislators and taxpayers scrutinize expenditures and search for increased value for hard-earned tax dollars, technical excellence and timely reports are not enough. OSA must provide audits in the most efficient manner, and we must dramatically change the way audits are conducted. What’s the goal? Improve efficiency and effectiveness without sacrificing quality.

Our potential for major productivity gains largely resides in the skills and attitudes of our people. As a result, our auditors need to continuously seek ways to eliminate inefficiencies and efforts that don't add value. To succeed, they must be adequately trained and work in a culture that promotes and rewards this behavior.
To reach these goals OSA will be engaging Audit Watch Inc., a group who specializes in the design, training, and implementation of change programs for accounting firms, to lead this project. OSA has the unique opportunity, with Audit Watch's assistance, to prove gains public accounting firms have achieved can be duplicated or even improved on by government entities.
Anticipated Benefits:

- Improved Efficiency
- Enhanced Client Service to Legislators and Citizens
- Improved Audit Quality
- Higher Staff Morale

Chapter 2 – Current Situation and Desired State of Major IT Applications/Infrastructure Assets

A. Current Applications/Services

1. Air Defense

Air Defense is an aggressive fulltime watchdog of any and all wireless activity around OSA. The objective is to add a strong layer of defense protecting wireless communications used by auditors.

Application Roadmap	
Operational Requirements	AirDefense updates as needed for both the Appliance and Sensors.
Short Term (< six months)	Apply Updates as needed
Scheduled (1-2 years)	Apply Updates as needed Replace equipment if required
Planned	Replace server both appliance and sensors as required

2. E-Learning

The LearningServer for SharePoint (LSS) Learning Management system and new SharePoint platform will enable our office to become a certifiable organization that is basically a virtual university in which auditing employees can register, receive training,

submit tests, communicate with others, and receive certification over the Internet. It will also incorporate interactive components (multimedia, email, chat, Web site hyperlinks, discussion rooms, instructor Q & A) in a self paced, robust learning environment.

LearningServer is a vendor-customized Windows SharePoint Services website.

Application Roadmap	
Operational Requirements	Periodic backups, restores based on user requests. Server Security updates.
Short Term (< six months)	Acquisition of additional backup and recovery tools.
Scheduled (1-2 years)	Continued development of training content and user enrollment.
Planned	Migration of client software from Office 2003 to Office 2007.

3. Electronic Publication System (EPS)

The Electronic Publication system supports the agency mission by providing a subscription and notification mechanism for publishing Audit Reports and press releases.
The EPS system is an application component of the public website. The Electronic Publication System (EPS) allows interested parties to sign up for reports that meet their selection criteria. Audit reports are automatically distributed to registered users when released.

Application Roadmap	
Operational Requirements	Server Security updates.
Short Term (< six months)	Ad hoc changes based on requests from OSA Administrative staff
Scheduled (1-2 years)	Maintain
Planned	Maintain

4. Exchange 2003 Enterprise Server (Email)

Manages both in and out bound email for OSA users

Application Roadmap	
Operational	Apply Microsoft updates as needed for both the email server and

Requirements	OS.
Short Term (< six months)	1. Create and delete accounts as required. 2. Apply Updates as needed.
Scheduled (1-2 years)	1. Create and delete accounts as required. 2. Apply Updates as needed. 3. Replace equipment if required.
Planned	Replace server both hardware and software as required.

5. External Website

The public website supports the agency mission by providing the mechanism for publishing Audit Reports

Application Roadmap	
Operational Requirements	Adding articles to the front page newsroom. Server Security updates.
Short Term (< six months)	Ad hoc style changes relating to the appearance and content of the website.
Scheduled (1-2 years)	Maintain
Planned	Maintain

6. Grants Information Center (GIC)

The GIC is an automated system to capture non-government organization grant information. The information will be maintained in a data mart designed to enable end user analysis and timely reporting of data. The system will provide a tool to more effectively and efficiently oversee the grants awarded to non-government organizations. The new system will improve efficiency and accuracy in the following areas:

• Reporting to the State Legislature, Grantee Agencies, and the general public.
• OSA compliance determination and auditing of grants
• As a result OSA should be able to reallocate staff resources from manual reporting to perform on-site reviews/audits

The system utilizes the ITS Data Warehouse Services (DWS) for data storage and reporting. All aspects of the application are hosted at ITS (this includes web hosting (https://www.grants.ncauditor.net/Portal/displayLogon.do), data storage in SAS as well as user authentication via NCID.

Application Roadmap	
Operational Requirements	All reports are generated nightly via a scheduled job at ITS. Monthly, all data is demoted from the production environment to both QA and Dev (requires ITS Incident ticket)
Short Term (< six months)	Heavy enhancement activity will continue to occur. See GIC_Enhancements_List.doc
Scheduled (1-2 years)	Continued enhancement including: - The system needs to be linked with NCAS to automatically download grant disbursements. (Currently done manually) - Comprehensive list of reports for each grantee via links (to make system more user friendly)
Planned	- Integration with Beacon Grants module - Integration with Secretary of State tax id database

7. Network Security

Secure the Network both internal and external (traveling audit teams) so that Auditors can issue non-qualified audits.

Application Roadmap	
Operational Requirements	Switches, firewalls, vpn concentrators, etc must be upgraded to new software as released by vendors. Schedule is determined by vendor releases and degree of criticality of patch and other ongoing priorities.
Short Term (< six months)	Maintain current architecture
Scheduled (1-2 years)	Maintain current architecture
Planned	Developed plans to upgrade all outdated switches and routers of OSA internal network was shelved as the budget was not approved.

8. Non-Governmental Organizations

The NGO System is used to capture non-government organization grant information. This information is used to produce the monthly Noncompliance list as mandated by GS 143C-6-23

Application Roadmap	
Operational Requirements	None
Short Term (< six months)	No additional development or maintenance is planned. System will be retired once the GIC system is fully functional
Scheduled (1-2 years)	No additional development or maintenance is planned. System will be retired once the GIC system is fully functional
Planned	RETIRED

9. Numara Track-IT!

The system is intended to provide an overall help desk solution to the end users while providing a database of history problems/solutions for the help desk team

Application Roadmap	
Operational Requirements	None
Short Term (< six months)	Complete implementation
Scheduled (1-2 years)	Updated as necessary
Planned	Update as necessary

10. Remote Desktop Deployment through Active Directory Policies and Windows Server Update Service (Remote Deployment)

Deployment of software to remote desktop users.
Remote Deployment of ACL and AS2. Utilizing WIN batch and patch link server

Application Roadmap

Operational Requirements	Apply Microsoft updates as needed for both the email server and OS.
Short Term (< six months)	Apply Updates as needed
Scheduled (1-2 years)	1. Apply Updates as needed. 2. Replace equipment if required.
Planned	Replace server both hardware and software as required.

11. State Auditors Resource Area (SARA) Intranet Portal

The SARA portal is an installed instance of Microsoft Office SharePoint Server (MOSS) 2007 Service Pack 1. The portal is for internal (intranet) use. It facilitates collaboration, workflow, and information sharing for staff of the Office of the State Auditor.

Application Roadmap	
Operational Requirements	Periodic backups, restores based on user requests. Server Security updates.
Short Term (< six months)	Acquisition of additional backup and recovery tools.
Scheduled (1-2 years)	Continued phased migration of other content sources.
Planned	Migration of client software from Office 2003 to Office 2007.

12. Time Reporting System (TRS)

Application provides time reporting and management for all OSA employees and provides billing information for cost recovery.

Application Roadmap	
Operational Requirements	Update the Holiday listings for coming calendar years for State Holidays. Insert or maintain time accounting (Auditing) Codes Periodic backups, restores based on user requests. Server Security updates.
Short Term	Make corrections to leave and time approvals as requested by

(< six months)	Budget Office.
Scheduled (1-2 years)	Maintain
Planned	Access how functions can be rolled into another system (BEACON).

B. Infrastructure Assets

1. Refresh older computers and infrastructure with up to date technology.
2. Completely rework of all external OSA network traffic to conform to ITS policy while enabling end to end data encryption to ensure data integrity.
3. Replace aging and unsupported network switching infrastructure (Nortel Switches)
4. Microsoft Enterprise Agreement / Server Software Refresh
    a. Replace/refresh existing Microsoft office, productivity and server software to ensure standardization, maintain compliance and ease administrative and support issues. These include:
        i. Enterprise Server – Refresh OSA MS Enterprise Server
        ii. Exchange Server – Refresh OSA Exchange Server
        iii. Install and configure SharePoint server in support of SARA project
        iv. SQL Server – Refresh SQL server
        v. MS Office - Refresh office and productivity software to latest versions from Microsoft.
5. Improve wireless networking security to provide both offensive and defensive network security.
6. Improve computer security for field auditors by providing data center access to critical applications so that in event of theft or loss data will not be compromised.

C. Operations/IT Management

1. Move towards an ITIL based, service orientated IT organization
2. Improve Project Management and Delivery (UMT PPM Tool)
3. Improve Applications Portfolio Management (UMT APM Tool)
4. Improve Infrastructure assets management and inventory control (Numera)
5. Improve Security management by implementing a network monitoring tool to monitor network traffic and application response.
6. Improve Disaster recovery and business continuity planning (LDRPS Software)

D. Human Resources

MIS Staff

CIO (Lenny Superville, Phd Applied Math Operations Research /Industrial Engineer)
Technology Support Analyst (Michael Fetting)
Technology Support Specialist (Leo Alls)
Business and Technology Applications Analyst (Neelema Chitoor)
Business and Technology Applications Specialist (Mark Smith)
Business and Technology Applications Specialist (Gary Hinkel)
Network Specialist (Paul Saksa)

Chapter 3 – IT Initiatives Developed From and Aligning With Plan Drivers

Initiative: Infrastructure Upgrades (Nortel Switches)	
Summary	In early 1997, Nortel began shipping a core networking product called the Accelar 1200. This product along with other Nortel products distributed throughout the Auditor building became the core foundation for the data networking infrastructure. While these products have been extremely reliable for the last 9 years, their lifecycle has ended. The ITS standard for updating this type of equipment is a much shorter 5 years. On November 30th, 2006 the Accelar 1200 product will not have a support option available from Nortel. This means that if there is a failure of hardware or software on the product, significant downtime is likely. Nortel proposes that the N.C. State Auditor updates the equipment in the network to avoid this downtime as well as make security enhancements to the network infrastructure.
Objectives	• Replace outdated Nortel Switches • Increase security on all internal networks up to port level inspections. Currently two options are being considered: *Option 1:* Replace the core Accelar 1200 with 2 Nortel ERS5530 switches. Replace the Baystack 450 switches in the closets with Nortel ERS5510 switches. Provide dual fiber paths from each of the closets distributed across the core ERS5530s. Put in place a Nortel technology called Split Multi-Link trunking (SMLT) at the core. *Benefits:* No Single Point of Failure in the Network means 99.999% uptime. Nortel has provided for redundant fiber connections from each closet in the building back to the core closet. This means that any fiber module or physical pair of fiber itself from any closet can have a failure and the network stays operational. Closet

	switches are connected together in a fashion we call "resilient stacking". This means that if any switch in a stack has an outage, only the users on the ports on that switch are affected. The rest of the users on the network are not affected. In addition, Nortel is splitting the connections from each closet across 2 core switches utilizing a technology called SMLT. As networks grow ever more critical, there is an increasing demand for multiple paths from all wiring closet switches into the core of the network to eliminate all single points of failure. Nortel's SMLT technology allows for no single point of failure on the network. Some vendor solutions utilize an aging protocol called Spanning Tree to provide network redundancy. Spanning Tree only allows for one link from each closet to be active at any one time. SMLT allows for both links to be active, doubling throughput. In case of a network outage of either core switches, SMLT allows for the network to failover in less than 1 second (average time is 0.4 seconds). Spanning tree fails over in at least several seconds. This type of delay would be enough to frustrate users using real time media (voice or video) and could be long enough to reset IP phones. Minimizing down time during scheduled network maintenance, such as system upgrades or configuration changes, is also a key requirement of today's networks. Providing network operators with tools that allow them to apply network changes during working hours, rather than after hours, can lead to significant cost savings over time. The Nortel SMLT solution provides a simple way of upgrading aggregation/core devices without impacting overall network availability. Increasing the speed of the network means more productivity. Using SMLT technology, Nortel can double the bandwidth from each closet (1GB to 2GB) to the core of the network resulting in higher throughput. In addition, the switches used in this design are 10 times faster than the switches N.C. Auditor is using today. Security is in the DNA. Security enhancements are inherent to the products. Better security means secure information won't be compromised. Nortel has features built into the solution that provide for enhanced security over what is currently used. Features like SSHv2, 802.1x, and SNMPv3 are standard in Nortel's products. Having the latest technology means N.C. Auditor can support even more enhanced security features both now and in the future. *Option 2:* Add Power over Ethernet Capabilities Power over Ethernet (PoE) technology provides power and data connectivity to devices such as IP phones, wireless access points, network cameras, security and lighting devices, and access control devices (i.e. badge readers). According to IDC's Worldwide Power over Ethernet 2004-2008 Forecast and Analysis report, the Power over Ethernet market revenue is expected to grow at an 8.9 percent CAGR (compound annual growth rate) over the next five years. Benefits: Purchasing this capability now means you'll avoid costly retrofitting later.

	Many network devices are becoming powered over Ethernet cable instead of through power outlets (wall outlets). If N.C. Auditor believes at some point that technologies listed above will be used in the network, purchasing PoE switches will avoid costly retrofitting of network devices later. In addition, NC Auditor will have these capabilities from day 1, which will make the time to roll out new services shorter. Retrofitting devices for PoE later means adding points of failure in the network. Additional points of failure means downtime and loss of productivity. If NC Auditor must retrofit for PoE capabilities later, either powered patch panels or PoE injectors must be used. This will add multiple points of failure into the network which inevitably will result in downtime and loss of productivity. *Add-On capabilities:* Endpoint Security: Adding Nortel's Secure Network Access (NSNA) means NC Auditor can verify key attributes of every device on the network to protect assets at the most vulnerable point of entry – the network edge. A key element described in the Nortel Layered Defense posture is endpoint security. The network edge is no longer where the corporate firewalls are. A paradigm shift has pushed the network edge to where the user and their computing device are located. The road warrior connecting to the corporate network can have secure remote access to your network. Organizations are extending their firewall to the corporate network to increase protection for critical computing resources such as data centers and mission-critical applications. According to ESG Research 2005 report, 43% of survey correspondents confirmed that their Internet worms/virus had been "carried in on an employee laptop". Securing these devices is integral to the defensive posture as most enterprises have more users than servers. Critical to managing these systems are security policies specifying enterprise configurations. Security policies include antivirus software, personal firewall software and enterprise configurations, such as disallowing noncompliant network applications. Controlling what devices are permitted to connect to the network provides significant protection. Does an enterprise really know what is connected to their network? Enterprise-provided systems, employees' personal devices, contractors, consultants and vendor support personnel all have devices which may be connected at any given time. Limiting network access to only authorized systems is essential. Nortel SNA addresses endpoint security, and implements automated configuration and security policy enforcement, increasing access control and risk mitigation. Nortel SNA, featuring our Tunnel Guard technology, checks to ensure the latest anti-virus, firewall applications, or software patches are running before authorizing users. All system elements can be evaluated including the operating system, patches, anti-virus software, personal firewall status, registry settings and other components. Verifying compliance and blocking connections from non-compliant systems can provide 100 percent compliance with corporate policy.

	Threat Protection: If there is vulnerability in the network, NC Auditor needs to know about it as soon as the threat is detected so the threat can be mitigated as soon as possible so key assets are not compromised. Nortel's Threat Protection System (TPS) detects, reports, blocks, and reports on any security event in the network.
Time Frame	4th Quarter 2008
Resources Involved	HR: Network Specialist Nortel Support Services *See Attachment: Nortel Replacement2008*
Costs	Total Solution (Hardware+Services): $92266.14 Total Recurring Maintenance: $14406 *See Attachment: Nortel Replacement*

Initiative: Disaster Recovery	
Summary	During annual testing/review of disaster recovery procedures and processes it came to light that not all of our applications are currently adequately backed up. While all of our data is backed up and recoverable, several components of our infrastructure are either unrecoverable or would require extensive effort to recover. It is recognized that in order to resume business as usual, both the infrastructure and data would need to be recovered. In addition, OSA must recognized the sensitive and confidential nature of the data residing on Agency servers and within Agency applications. Thus, any DR solution implemented must ensure the security and integrity of the systems being stored.
Objectives	A comprehensive and integrated disaster recovery solution needs to be developed that allows the agency to meet both Recovery Time Objectives and Recovery Point Objectives.
Time Frame	4th Quarter 2008
Resources Involved	HR: Network Specialist Technology Support Specialist Business and Technology Applications Specialist
Costs	Total Solution (Hardware+Services): $150000
